НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

«На правах рукопису»
УДК 519.21

«До захисту допущено»
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
“15” травня 2018р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 113 «Прикладна математика»

на тему: Визначення мінімальної кількості блоків підтвердження, що гарантує збереження транзакцій в блокчейні з заданою імовірністю у мережі з поганою синхронізацією і з корумпованим зловмисником

Виконав (-ла): студент (-ка) 2 курсу, групи _____ФІ-63М_____
(шифр групи)

Чоп Марина Миколаївна

Керівник д.т.н. Ковальчук Л.В.

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент д.т.н. Архіпов О.Є.

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018року

РЕФЕРАТ

Об'єм роботи 51 сторінка, 7 рисунків, 3 таблиці, 24 літературних посилань.

Об'єктом дослідження є ланцюжок блоків транзакцій на прикладі криптовалюти Bitcoin.

Метою даної дипломної роботи є визначення мінімальної кількості блоків підтвердження, що гарантує збереження транзакцій в ланцюжку блоків транзакцій з заданою імовірністю. Попередні роботи в даному напрямку не враховували час затримки поширення блоків у мережі.

Завдання дослідженя – розглянути структуру ланцюжків блоків транзакцій та криптовалюту Bitcoin, провести власний аналіз успіху атаки подвійних витрат із урахуванням часу поширення блоків у мережі та визначити мінімальної кількості блоків підтвердження для гарантування збереження транзакцій із заданою імовірністю.

БЛОКЧЕЙН, КРИПТОВАЛЮТА, BITCOIN, АТАКА ПОДВІЙНИХ ВИТРАТ, ТРАНЗАКЦІЯ.

ABSTRACT

The work contains 51 pages, 7 pictures, 3 tables, 24 references.

The subject of research is the blockchain on the example of crypto-currency Bitcoin.

The aim of this qualification work is to determine the minimum number of confirmation blocks, which guarantees the storage of transactions in the blockchain with a given probability. Previous work in this direction did not take into account the time delay of the distribution of blocks in the network.

The research task is to consider the structure of the blockchain and Bitcoin, to conduct a self-analysis of the success of the double-spending attack, taking into account the time of distribution of blocks in the network, and to determine the minimum number of confirmation blocks to guarantee the preservation of transactions with a given probability.

BLOCKCHAIN, CRYPTOCURRENCY, BITCOIN, DOUBLE-SPENDING ATTACK, TRANSACTION.

ЗМІСТ

Вступ 7
1. Ланцюжок блоків транзакцій 9
1.1 Ланцюжки блоків транзакцій 9
1.2 Поняття криптовалюти 15
Висновки до розділу 1 18
2. Криптовалюта Bitcoin та основні атаки. Аналіз Грюнспана та Накамото .. 19
2.1 Загальні відомості про систему Bitcoin 19
2.2 Основні атаки на криптовалюту Bitcoin 24
2.3 Аналіз Грюнспана та Накамото 27
Висновки до розділу 2 33
3. Визначення мінімальної кількості блоків підтвердження, що гарантує збереження транзакцій в блокчейні з заданою імовірністю 34
3.1 Основні припущення та допоміжні твердження 34
3.2 Ймовірність успіху атаки подвійних витрат в залежності від затримки прийняття блоків у мережі 39
3.3 Числові результати 45
Висновки до розділу 3 48
ВИСНОВКИ 49
ПЕРЕЛІК ПОСИЛАНЬ 50

ВСТУП

Актуальність роботи: після створення електронних платежів велика кількість людей почала ними користуватися через їхню зручність та надійність. Наразі в криптовалюти вкладені значні грошові ресурси, отже питання забезпечення функціонування та безпеки гостро стоїть в нинішньому суспільстві.

Об'єкт дослідження: ланцюжок блоків транзакцій на прикладі криптовалюти Bitcoin.

Предмет дослідження: стійкість ланцюжка блоків транзакцій до атаки подвійних витрат із урахуванням часу поширення блоку у мережі.

Метою роботи є: визначення мінімальної кількості блоків підтвердження, що гарантує збереження транзакцій в ланцюжку блоків транзакцій з заданою імовірністю у мережі з поганою синхронізацією та зкорумпованим зловмисником із урахуванням часу затримки поширення блоку у мережі.

У ході дослідження ставляться такі *завдання:*

- дослідження структури та принципу роботи ланцюжка блоків транзакцій, їх застосування у криптовалюті Bitcoin.
- огляд існуючих аналізів на стійкість ланцюжка блоків транзакцій щодо атаки подвійних витрат
- власний аналіз успіху атаки подвійних витрат із урахуванням часу поширення блоків у мережі
- числове та графічне зображення отриманих результатів

Наукова новизна одераних результатів полягає у розширенні існуючих результатів аналізу атаки подвійних витрат на ланцюжків блоків транзакцій на прикладі криптовалюти Bitcoin за рахунок врахування часу затримки поширення блоків у мережі.

Практичне значення одержаних результатів дає змогу вдосконалити створення нових та оновлення існуючих систем на основі ланцюжків блоків транзакцій на предмет стійкості до атаки подвійних витрат.

1. ЛАНЦЮЖОК БЛОКІВ ТРАНЗАКЦІЙ

В даному розділі буде розглянуто структуру ланцюжка блоків, який використовується для запису транзакцій в системі Bitcoin та подібних до неї. Також буде введено поняття криптовалюти та оглянуто основні її складові. Буде наведено описання системи функціонування деяких криптовалют, що мають різні структури.

1.1 Ланцюжки блоків транзакцій

Ланцюжок блоків транзакцій (англ. Blockchain, від block — блок, chain — ланцюг) — розподілена база даних, яка підтримує постійно зростаючий перелік записів, званих блоками, від підробки та переробки[1]. Кожен блок містить часову мітку та посилання на попередній блок хеш дерева.

Блок транзакцій — спеціальна структура для запису групи транзакцій в системі Bitcoin та аналогічних до неї. Щоб транзакція вважалася достовірною («підтвердженою»), її формат і підписи повинні перевірити і потім групу транзакцій записати в спеціальну структуру — блок. Інформацію у блоках можна швидко перевірити. Кожен блок завжди містить інформацію про попередній блок. Усі блоки можна вибудувати в один ланцюжок, який містить інформацію про всі вчинені коли-небудь операції. Перший блок в ланцюжку — первинний блок (англ. genesis block) — розглядається як окремий випадок, так як у нього відсутній батьківський блок. Блок складається із заголовку та списку транзакцій. Заголовок блоку включає в себе свій хеш, хеш попереднього блоку, хеши транзакцій та додаткову службову інформацію. Першою транзакцією в блоці завжди вказується отримання комісії, яка стане нагородою користувачеві за створений блок.

Розглянемо приклад блоку криптовалюти Bitcoin[2]. У системі Bitcoin службовий рядок перетворений у заголовок блоку, і включає в себе хеш попереднього блоку, кореневий хеш дерева Меркле з усіх транзакцій у блоці, поточний час та складність.

Нижче наведемо приклад блоку № 358782

Hash: 00000000000000000ff5737b9dfdad72c05b1b27dfee51a496d015f2e8e3e6bb

Previous block:
000000000000000000336310b668d7b652d5a324844d1e12262cd2a1812946966

Next block:
0000000000000000145186966c1bd610dfb6eb83dc107e95bb0829592ae7f935

Time: 2015-05-31 09:28:15

Difficulty: 48 807 487 244.681384 ("Bits": 181686f5)

Transactions: 158

Total BTC: 2011.57132216

Size: 249.043 kilobytes

Merkle root:
41c77aa3df7d98487db4cd9f3aa9ce9c73c54c1f72dc72c8d7fc70c0b36fbaac

Nonce: 1552980181

Заголовок блоку містить такі поля:

Таблиця 1.1 – Заголовок блоку

Поле	Значення	Оновлюється коли	Розмір (байт)
Version	Версія блоку	Виходить нове ПО	4
hashPrevBlock	256-бітний хеш попереднього заголовку блоку	Надходить новий блок	32
hashMerkleRoot	256-бітний хеш, оснований на усіх транзакціях в блоці	Транзакція приймається	32
Time	Поточний час в секундах з 1970-01-01T00:00 UTC	Кожні декілька секунд	4

Bits	Поточна складність	Приймається складність	4
Nonce	32-бітне число (починається з 0)	Хеш не підійшов (інкремент)	4

Далі йдуть всі або деякі з останніх транзакцій, які ще не були записані в попередні блоки. Для транзакцій в блоці використовується тип хешування під назвою “дерево Меркл”[3], який зображений на рисунку 1.1. За цим типом хешування дані поділяються на блоки, які індивідуально хешуються на нижчих рівнях (наз. Leaf Tiger Hash), потім з кожної пари хешів по черзі отримуємо хеш вищого рівня (Internal Tiger Hash). Якщо для хеш-значення нема пари, він переноситься на вищий рівень без змін. Це продовжується доки не отримаємо один останній хеш, який називається Tiger Tree Root.

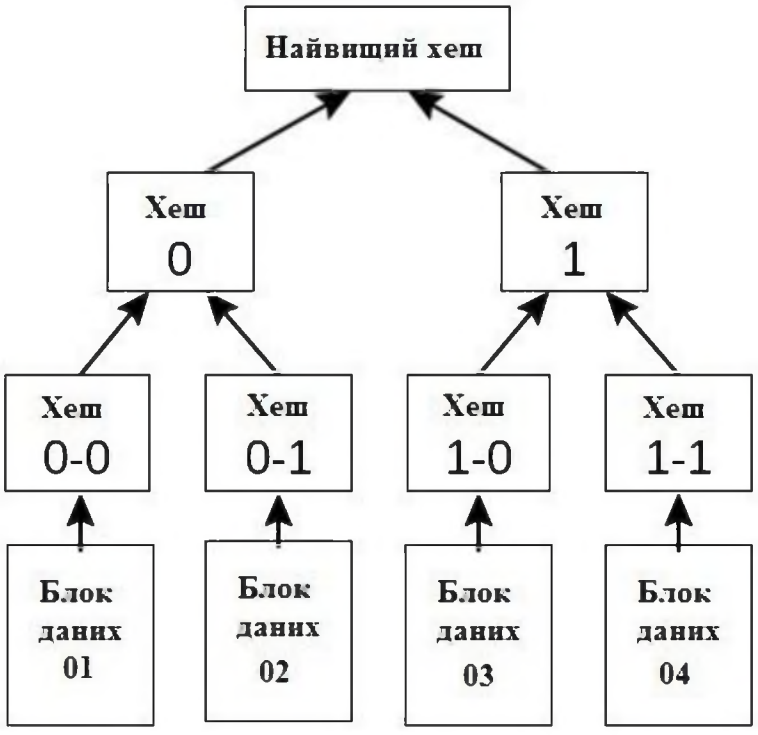

Рисунок 1.1 Дерево Меркл

Створений блок буде прийнятий іншими користувачами, якщо числове значення хешу заголовка дорівнює або нижче певного числа, величина якого періодично коригується. Так як результат хешування непередбачуваний,

немає алгоритму отримання бажаного результату, крім випадкового перебору. Якщо хеш не задовольняє умові, то довільно змінюється частина службової інформації в заголовку і хеш перераховується. Зазвичай потрібна велика кількість перерахунків. Коли варіант знайдено, вузол розсилає отриманий блок іншим підключеним вузлам, які перевіряють блок. Якщо помилок немає, то блок вважається доданим в ланцюжок і наступний блок повинен включити в себе його хеш.

Блоки одночасно формуються безліччю «майнерів»[4]. Блоки, які задовольняють критеріям, відправляються в мережу, включаючись в розподілену базу блоків. Регулярно виникають ситуації, коли декілька нових блоків в різних частинах розподіленої мережі називають попереднім один і той же блок, тобто ланцюжок блоків може розгалуджуватися (рис. 1.2). Спеціально або випадково можна обмежити ретрансляцію інформації по нових блоках (наприклад, одна з ланцюжків може розвиватися в рамках локальної мережі). У цьому випадку можливе паралельне нарощування різних гілок.

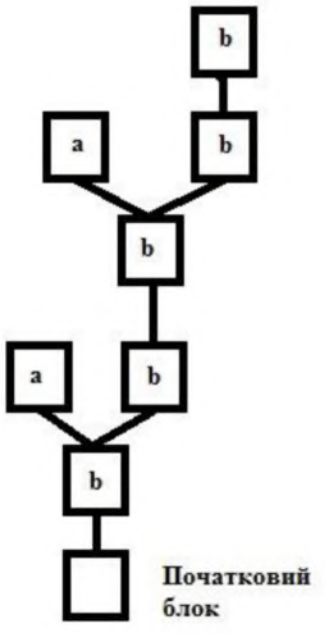

Рис. 1.2 Ланцюжок блоків транзакцій

У кожному з нових блоків можуть зустрічатися як однакові транзакції, так і різні, які увійшли тільки один з них. Коли ретрансляція блоків поновлюється, майнери починають вважати головним ланцюжок з урахуванням рівня складності хешу і його довжини. При рівності складності і довжини перевага віддається тому ланцюжку, кінцевий блок якого з'явився раніше. Транзакції, що увійшли тільки у відхилену гілку (в тому числі по виплаті винагороди), втрачають статус підтверджених.

Якщо це операції з передачі біткойнів, то вони будуть поставлені в чергу і потім включені в черговий блок. Транзакції отримання винагороди за створення відхилених блоків не дублюються в іншій гілці, є «зайві» біткойни, виплачені за формування відкинутих блоків, не отримують подальших підтверджень і “втрачаються”.

Розподілена база даних Blockchain формується як безперервно зростаючий ланцюжок блоків з записами по всіх транзакціях. Копія бази даних або її частини одночасно зберігається на безлічі комп'ютерів та синхронізуються відповідно формальним правилам побудови ланцюжка блоків. Інформація в блоках не шифрована і доступна у відкритому вигляді, але захищена від змін криптографічно через хеш-ланцюжок.

Найчастіше умисна зміна інформації в будь-якій з копій бази або навіть в досить великій кількості копій не буде визнана істинною, так як не відповідатиме правилам. Деякі зміни можуть бути прийняті, якщо будуть внесені в усі копії бази (наприклад, видалення кількох останніх блоків через помилку в їх формуванні).

Підтвердження транзакцій. Поки транзакція не включена в блок, система вважає, що кількість біткойнів на певній адресі залишається незмінною. У цей час є технічна можливість оформити кілька різних транзакцій по передачі з однієї адреси одних і тих же біткойнів різним

одержувачам[5]. Але як тільки одна з подібних транзакцій буде включена в блок, інші транзакції з цими ж біткойнами система буде вже ігнорувати.

Наприклад, якщо в блок буде включена більш пізня транзакція, то більш рання буде вважатися помилковою. Є невелика ймовірність, що при розгалудженні дві подібні транзакції потраплять в блоки різних гілок. Кожна з них буде вважатися правильною, лише при відмиранні гілки одна з транзакцій стане вважатися помилковою. При цьому не буде мати значення час здійснення операції.

Таким чином, попадання транзакції в блок є підтвердженням її достовірності незалежно від наявності інших транзакцій з тими ж біткойнами. Кожен новий блок вважається додатковим підтвердженням транзакцій з попередніх блоків. Якщо в ланцюжку 3 блоку, то транзакції з останнього блоку будуть підтверджені 1 разів, а вміщені в перший блок буде мати 3 підтвердження. Досить дочекатися декількох підтверджень, щоб звести ймовірність скасування транзакції до мінімуму.

Для зменшення впливу таких ситуацій на мережу існують обмеження на розпорядження щойно отриманими біткойнами. Згідно сервісу blockchain.info до травня 2015 року максимальна довжина відкинутих ланцюжків була 5 блоків. Необхідне число підтверджень для розблокування отриманого залежить від програми-клієнта, або від вказівок приймаючої сторони. Клієнт «Bitcoin-qt» для відправлення не вимагає наявності підтверджень, але у більшості одержувачів за замовчуванням виставлено вимогу 6 підтверджень, тобто реально скористатися отриманим зазвичай можна через годину. Різні онлайн-сервіси часто встановлюють свій поріг підтверджень.

1.2 Поняття криптовалюти

Цифрова валюта – це засіб обміну, який працює як валюта у певному середовищі, але не має усіх атрибутів реальної валюти. Іншими словами, віртуальна валюта або має еквівалентне значення в реальній валюті або діє як замінник реальної валюти.[6]

Криптовалюта – це вид віртуальної валюти, яка використовує методи асиметричної криптографії для забезпечення безпеки транзакцій та контролю створення нових монет.[7] До середини 2013 року програмне забезпечення всіх криптовалют, крім Ripple, базувалося на відкритому коді системи Bitcoin. З 2013 року почали з'являтися криптовалюти на інших розроблених платформах, які могли підтримувати біржову торгівлю, магазини та інше. Криптовалюти проектуються таким чином, щоб було неможливо повернути платіж, примусово заморозити або зняти кошти з гаманця без доступу до приватного ключа власника.[7]

Хоча використання криптографії з метою забезпечення конфіденційності платежів почала використовуватися з 1990 року [8], вперше термін "криптовалюта" почали використовувати після створення платіжної системи Bitcoin, яка була розроблена 2009 року людиною (або групою людей) під псевдонімом Сатосі Накамото (Satosi Nakamoto), [9] і використовує хешування SHA-256 та систему підтвердження виконання роботи (англ. Proof-of-work).[10]

Спочатку криптовалютами майже ніхто не користувався і вони не мали вартості, угоди були рідкими та епізодичними. Восени 2009 року 1 BTC мав вартість в 0.8 центів і з тих пір біржовий курс почав підійматися вище 20000$ і падати назад до 5000$.

Пізніше почали з'являтися інші криптовалюти, які не залежали від Bitcoin, які називають форками Bitcoin. Приведемо декілька прикладів таких валют:

- Namecoin – децентралізована DNS, яка використовує криптовалюту цієї ж назви для реєстрації доменів .bit;[11]
- Litecoin – використовує хешування Scrypt, збільшений об'єм емісії та зменшений час підтвердження транзакції;[12]
- PPCoin – використовує механізм, утворений поєднанням систем підтвердження proof-of-work та proof-of-stake (часткове підтвердження), не має обмеження на загальний об'єм емісії; [13]
- Novacoin – аналогічна до PPCoin, але використовує Scrypt та зменшені коефіцієнти, пов'язані з емісією.

Процес генерування Bitcoin передбачає знаходження значення хеш-функції – процес випадковий та не несе в собі нічого корисного. Деякі криптовалюти врахували це і змінили процес майнінгу, додавши інші корисні цілі. Однією з таких форків є Primecoin.

Праймкойн (англ. Primecoin) – похідна криптовалюта від Bitcoin, але головна відмінність полягає у системі підтвердження виконання роботи: якщо Bitcoin використовує обчислення хешів за алгоритмом SHA-256, то система підтвердження праймкойн спирається на пошук великих простих чисел.

Послідовність Куннінгама поділяється на 2 типи:

- послідовність Куннінгама першого роду складає послідовність простих чисел, кожен член якої більший на 1 за подвоєний попередній;
- послідовність Куннінгама другого роду – це послідовність простих чисел, кожен член якої менший на 1 від подвоєного попереднього.

Розглянемо приклад з невеликими простими числами 5 та 7 та серединої 6.Подвоївши середину, маємо 12, де 11 та 13 знову пара простих чисел. Отже 5, 7, 11, 13 є послідовністю довжини 4. Її можна розділити на 5 та 11, які складають послідовність Куннінгама першого роду і, відповідно, 7 та 13 – послідовність другого роду.

Система праймкойн має 3 типи ланцюгів для прийняття як підтвердження виконання роботи: ланцюг Каннінгема 1-го роду, 2-го роду та bi-twin ланцюг. Зі збільшенням довжини ланцюга складність зростає в експоненціальному порядку, доки перевірка результату залишається в розумних межах. Згідно з протоколом PoW, робота повинна бути підтверджена на усіх вузлах мережі.

Перевірка відбувається за класичним тестом Ферма за основою 2 разом з тестом Ейлера-Лагранжа-Лифчитза. У системі не вимагається пряма перевірка простоти

Генерування послідовностей Куннінгама має велике значення для криптографічних систем, де використовується схема шифрування Ель-Гамаля. Ці дані використовуються там, де має місце проблема обчислення дискретного логарифму.

Також було створено багато інших форків, які не несуть в собі нічого нового, так як вони є або точною копією Bitcoin або різниця незначна і полягає у швидкості емісії та/або алгоритмом хешування.

Криптовалюти мають різне відношення та правовий статус в різних країніх. В певних країнах офіційно дозволені операції з біткойнами, в тому числі в якості платіжного засобу. В інших же країнах подібні операції заборонені або строго обмежені. Навіть в одній країні можна зустріти, коли різні державні установи відносяться до криптовалют по-різному.

Так, наприклад, національний банк Хорватії визналв криптовалюту Bitcoin законною, але його не слід розглядати як електронні гроші, тобто магазини не забов'язані приймати їх на рівні з місцевою валютою. [14] Норвегія притримується такої ж точки зору. Повністю Bitcoin був заборонений у Китаї національним банком 5 грудня 2013 року. В заяві вказано, що Bitcoin не є валютою в реальному сенсі цього слова. Фінансовим компаніям було заборонено будь-які операції, пов'язані з Bitcoin. У листопаді 2013 року в Сенаті США проходили слухання з приводу Bitcoin, в результаті яких було прийняте рішення не забороняти циркуляцію криптовалют а

працювати над врегулюванням цього бізнесу. [15] 25 березня 2014 року Служба внутрішніх доходів США випустила посібник по оподаткуванню операцій з Bitcoin та іншими криптовалютами. В деяких країнах і досі нема офіційного рішення щодо врегулювання і правового статусу Bitcoin.

Криптовалюти, зазвичай, мають децентралізоване управління і функціонування системи проходить децентралізовано в одноранговій мережі (англ. peer-to-peed, P2P – рівний до рівного). Як правило, має верхню межу загальної кількості емісії, хоча це не обов'язково і існують такі криптовалюти, як PPCoin, Novacoin та інші, які не мають фіксованого об'єму емісії.

Усі діючі на даний момент криптовалюти використовують псевдоанонімність – усі транзакції знаходяться у публічному доступі, але прив’язки до конкретної особи не мають. Однак, особистість власника може бути визначена при певних додаткових умовах. [16] Наразі йде створення криптовалюти Zerocoin, в якій планується повний перехід від псевдоанонімності до анонімності.

Рівний до рівного – це варіант архітектури системи, в основі якої є мережа, яка складається з рівноправних вузлів. У цій мережі кожен вузол є як клієнтом так і сервером.

Висновки до розділу 1

В даному розділі було розглянуто структуру ланцюжка блоків транзакцій системи Bitcoin та подібних до неї. Дана структура набуває все більшої популярності та поширюється в різні сфери нашого життя. Також було розглянуто основні складові криптовалюти.

2. КРИПТОВАЛЮТА BITCOIN ТА ОСНОВНІ АТАКИ. АНАЛІЗ ГРЮНСПАНА ТА НАКАМОТО

В даному розділі буде розглянуто основні положення криптовалюти Bitcoin, її складові та принцип функціонування. Також буде наведено аналіз стійкості до атаки подвійних витрат, який проводив Грюнспан у порівнянні з аналізом автора криптовалюти Сатосі Накамото.

2.1 Загальні відомості про систему Bitcoin

Bitcoin – це електронна платіжна система, створена програмістом або групою програмістів під іменем Сатосі Накамото (Satoshi Nakamoto), яка використовує однойменну розрахункову одиницю. Розробка почалася у 2007 році, у 2008 році був опублікований файл з описом протоколу а уже в 2009 році мережа Bitcoin була запущена.

У вересні 2012 року був заснований фонд "Bitcoin Foundation", який мав заявлені цілі "стандартизація, захист та заохочення використання криптографічних коштів Bitcoin на користь користувачів по всьому світу".[17] Одним із засновників цього фонду був і Сатосі Накамото. Фонд зареєстрований Службою внутрішніх доходів США в Сіетлі в якості благодійного фонду. Організаційна модель фонду розроблена по аналогії з "Linux Foundation" та фінансується в основному за рахунок грантів комерційних організацій, які залежать від технології Bitcoin.

Bitcoin першим представив можливість прямої передачі прав власності іншій персоні через Інтернет без участі зовнішніх гарантів, причому передача безпечна та надійна і ніхто не може її оскаржити, відсутня обов'язкова комісія за проведення операцій, будь які транзакції можуть відбуватися для

кожної із сторін безкоштовно. Дана система реалізована за принципом рівний-до-рівного (P2P), що дає змогу електронному платежу відбуватися без залучення третьої сторони-гаранта і жодна зі сторін не може відмінити, заблокувати або примусово провести угоду (транзакцію).

Однією з головних особливостей системи – повна децентралізація, нема центрального адміністратора або будь-якого аналога. Необхідним і достатнім елементом цієї платіжної системи є програма-клієнт, яка має відкрите програмне забезпечення. Запущені на великій кількості комп'ютерів програми-клієнти з'єднуються між собою в однорангову мережу, в якій кожен вузол рівноправний та самодостатній.

Біткойни (монети, BTC) існують у вигляді записів у розподіленій базі, в якій у загальному доступі зберігаються транзакції, які вказують на Bitcoin-адреси відправників та отримувачів, але не мають інформації про реальні дані їх власників.[18] В базі нема записів про поточну кількість біткойнів у власника.

Кожен користувач системи може генерувати необмежену кількість пар ключів (алгоритм ECDSA з параметром secp256k1). Основна ціль використання ключів – створення Bitcoin-адреси та підтвердження правомірності формування транзакцій. Розмір закритого ключ – 256 біт, а відповідного йому відкритого ключа – 512 біт.[19] Ключі зберігаються в шифрованому файлі *wallet.dat*. Для розпорядження біткойнами не обов'язково мати цей файл – в більшості випадків буде достатньо отримати лише закритий ключ.

Адресація біткойнів – створення умов подальшого розпорядження ними. Умови формуються за допомогою відкритого ключа, а для подальших операцій з біткойнами потрібен відповідний електронний підпис, отриманий за допомогою секретних ключів. Приклад Bitcoin-адреси: *1BQ9qza7fn9snSCyJQB3ZcN46biBtkt4ee*. Технічно, адреса представляє собою 160-бітний хеш від відкритого ключа ECDSA ключової пари.

Процес створення Bitcoin-адреси:

1. Береться відкритий ключ (65 байт, 1 байт 0x04, 32 байт відповідають координаті X, 32 байт відповідають координаті Y):
04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5f

2. Відбувається SHA-256 хешування відкритого ключа:
261c1eb21fc4708c6acbe1cfc6d4565652e9e768b620782898936b93000a6c02

3. Виконується RIPEMD-160 хешування результату SHA-256:
62e907b15cbf27d5425399ebf6f0fb50ebb88f18

4. Додається байт-ідентифікатор перед RIPEMD-160 хешем (0x00 для основної мережі)
0062e907b15cbf27d5425399ebf6f0fb50ebb88f18

5. Виконується SHA-256 хешування по розширеному результату від RIPEMD-160:
9b90f16de7f0e580c07735dac15ffe23e2f8f8e103914e509aa91913ffdb9fb6

6. Виконується SHA-256 хешування по попередньому SHA-256 хешу, результат буде являти собою контрольну суму:
c29b7d937e3049e279391e62fdf00c12def7444013ddf6215808d10e9f2d5996

7. Беруться перші 4 байти від отриманого хеша:
c29b7d93

8. Ці 4 байти контрольної суми із пункта 7 додаються в кінець розширеного RIPEMD-160 хеша із пункта 4. Це 25-байтова двійкова Bitcoin-адреса.
0062e907b15cbf27d5425399ebf6f0fb50ebb88f18c29b7d93

9. Результат пункта 8 конвертується в рядок base58 . Це найбільш часто використовуваний формат bitcoin-адреси.
1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

Угоди перевіряються мережевими вузлами, утворюють блок та записуються у ланцюг блоків. [20] Цей процес генерування називається

майнінг (англ. mining). Емісія монет відбувається цим же процесом як винагорода за витрачені ресурси для генерування блоку. Обсяг емісії алгоритмічно обмежений так, щоб загальна кількість емітованих Bitcoin не перевищила 21 мільйон.

Транзакція Bitcoin – це підписаний розділ даних, який транслюється в мережу і записується в блоки. Вона посилається на попередні транзакції та переводить певну кількість Bitcoin-монет на зазначений відкритий ключ (Bitcoin-адресу). [21] Попередня транзакція стає входом для поточної транзакції, роль виходу слугує публічний ключ або Bitcoin-адреса одержувача. Транзакція відправляється по відкритим каналам у мережу, де її перевіряють вузли для додавання до поточного блоку.

Кроки роботи мережі є наступні:

1) Нові угоди транслюються на всі вузли.

2) Кожен вузол збирає нові транзакції в блок.

3) Кожен вузол працює над пошуком потрібного значення хешу (доведення виконаної роботи) для цього блоку.

4) Коли вузол знаходить доведення роботи, він передає блок до всіх вузлів.

5) Вузли приймають блок тільки тоді, коли всі операції у ньому дійсні і вже не проводяться.

6) Вузли підтверджують блок і працюють над наступним блоком в ланцюзі, використовуючи хеш прийнятого блоку.

Біткойни можуть передаватися через транзакції будь кому, хто повідомить коректну Bitcoin-адресу або відкритий ключ. Мінімальна величина, яку можна передати, становить 10^{-8} BTC. Окрім кількості монет та адреси, транзакція містить в собі хеш попередньої транзакції, за якою ці біткойни були отримані. Ця попередня транзакція вважається входом транзакції, а адреса одержувача – виходом. У кожної транзакції може бути декілька входів та/або виходів (рис. 2.1)

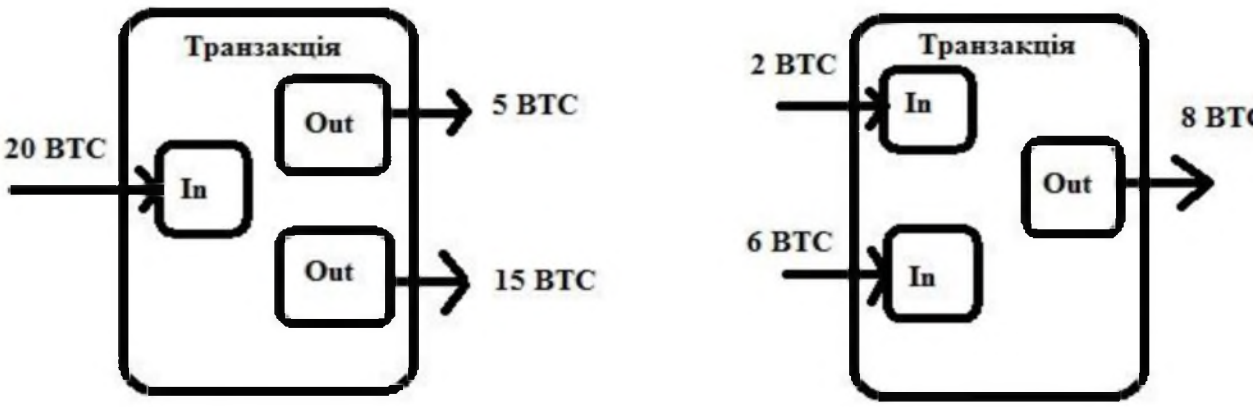

Рис. 2.1 – Приклад декількох входів та виходів у транзакціях.

Щоб транзакція вважалася підтвердженою, вона повинна перевіритися і бути доданою в групу транзакцій – блок.

Особливістю протоколу є те, що неможливо взяти лише деяку частину біткойнів із входу. Вони усі розподіляються по виходам, тобто якщо на адресу прийшло 2 біткойна однією транзакцією, то при наступній операції з цими монетами автоматично буде передаватися 2 біткойна. Якщо ж потрібно передати лише частину цих біткойнів, можна вказати свою адресу як одну з адрес отримувачів.

Кожен блок завжди має свій порядковий номер та хеш попереднього блоку. Взявши усі блоки, можна побудувати ланцюг блоків – відкриту базу, у якій зберігається інформація про усі транзакції біткойнів.

При одночасному створенні двох блоків для одних і тих же транзакцій вузлом приймається той, який перший до нього дійшов. Прийматися мережею буде той блок, для якого буде знайдено і оголошено наступний.

Блок складається із заголовка блока та списку транзакцій. Для транзакцій в блоці використовується тип хешування під назвою “дерево Меркла”[44], яке описано у попередньому розділі.

За цим типом хешування дані поділяються на блоки, які індивідуально хешуються на нижчих рівнях (наз. Leaf Tiger Hash), потім з кожної пари

хешів по черзі отримуємо хеш вищого рівня (Internal Tiger Hash). Якщо для хеш-значення нема пари, він переноситься на вищий рівень без змін. Це продовжується доки не отримаємо один останній хеш, який називається Tiger Tree Root. Саме це значення хешу використовується в P2P мережі.

В системі Bitcoin усі транзакції публічна, зберігаються у відкритому доступі, а секретність досягається відсутністю персоніфікації власників адрес. У 2011 році було показано, що на основі загальнодоступної інформації можна зв'язати велику кількість ключів як один з одним, так і з певною зовнішньою ідентифікуючою інформацією.

2.2 Основні атаки на криптовалюту Bitcoin

Атака гнучкості – це вид атаки, який дозволяє змінити унікальний ідентифікатор транзакції біткойнів до її підтвердження у мережі. У Bitcoin гнучкість транзакцій описує те, що підписи, які підтверджують право власності на біткойни, передаються в транзакції та не мають жодної гарантії цілісності них самих. Це дозволяє побудувати атаку гнучкості, в якій транзакція перехоплюється, модифікується і транслюється в мережу, в результаті чого система вважає, що первісна операція не була підтверджена.[22]

Атаки гнучкості відрізняється від атаки подвійних витрат. Атакуюча сторона вже не є стороною, яка ввела транзакцію, а є приймаючою стороною. Атакуючий викликає транзакцію на переведення коштів на свій рахунок. Потім очікується транслювання транзакції в мережу. Після того, як була отримана копія транзакції, вона модифікується щоб змінити підпис без порушення її. Модифікована транзакція потім транслюється в мережу. Будь-яка з двох транзакцій може бути пізніше підтверджена. Атака гнучкості вважається успішною, якщо модифікована версія угоди згодом підтвердилася.

Sybil-атака. Sybil-атака полягає у створенні атакуючою стороною великої кількості робочих частин (аккаунтів) мережі та використанні їх у своїх цілях.[23] Вразливість системи до даного типу атаки залежить від того, наскільки просто та "дешево" можна створювати ці складові.

При атаці мережа Bitcoin заповнюється великою кількістю вузлів, які контролює атакуюча сторона з метою відділення певної кількості інших вузлів мережі в підмережу. Хоча Bitcoin не дає повної ізоляції вузлів у мережі, вони можуть використовуватися для інших атак.

Наведемо декілька шляхів використання цієї слабкості:

- атакуючий може відмовитися передавати створені блоки і транакції від усіх контрольованих вузлів, що призводить до сповільнення або відключення від мережі;
- є можливість передавати лише створені ним блоки, обмежуючи певну адресу в окремий під мережу (ланцюг). Це відкриває шлях до атаки подвійних витрат;
- якщо використовуються транзакції з 0 підтвердженнями, то атакуючий може відфільтрувати певні транзакції, щоб провести атаку подвійних витрат;
- шифрування або анонімність з низькою затримкою передачі угод Bitcoin може бути зламане за допомогою часової атаки (timing attack), якщо джерело транзакцій підключене до декількох вузлів атакуючого і він може спостерігати за транзакціями.

Атакою подвійних витрат називається вдале використання одних і тих же засобів двічі. Bitcoin має вразливість до цієї атаки на початковому етапі знаходження транзакції в мережі. Чим більше у транзакції підтверджень, тим менше ризик того, що вона буде використана декілька разів.

Коли здійснюється транзакція за біткоіни, то очікується, що після перерахування монет відправник отримує у відповідь продукт або послугу, за яку він сплатив. Атака «**double-spending**» (подвійні витрати) - це атака, яка полягає в тому, що спочатку продавець переконується в тому, що транзакція

на оплату була проведена, після чого він передає свій товар, а після отримання товару покупцем створюється нова транзакція, яка і приймається мережею Bitcoin замість першої.

Ланцюжок блоків можна представити у вигляді дерева, що починається з початкового блоку і йде послідовно. Гілки цього дерева являють собою історії транзакцій. Гілка не може утримувати двох конфліктних транзакцій, однак може бути інша гілка, яка містить суперечливу транзакцію (рис. 2.2).

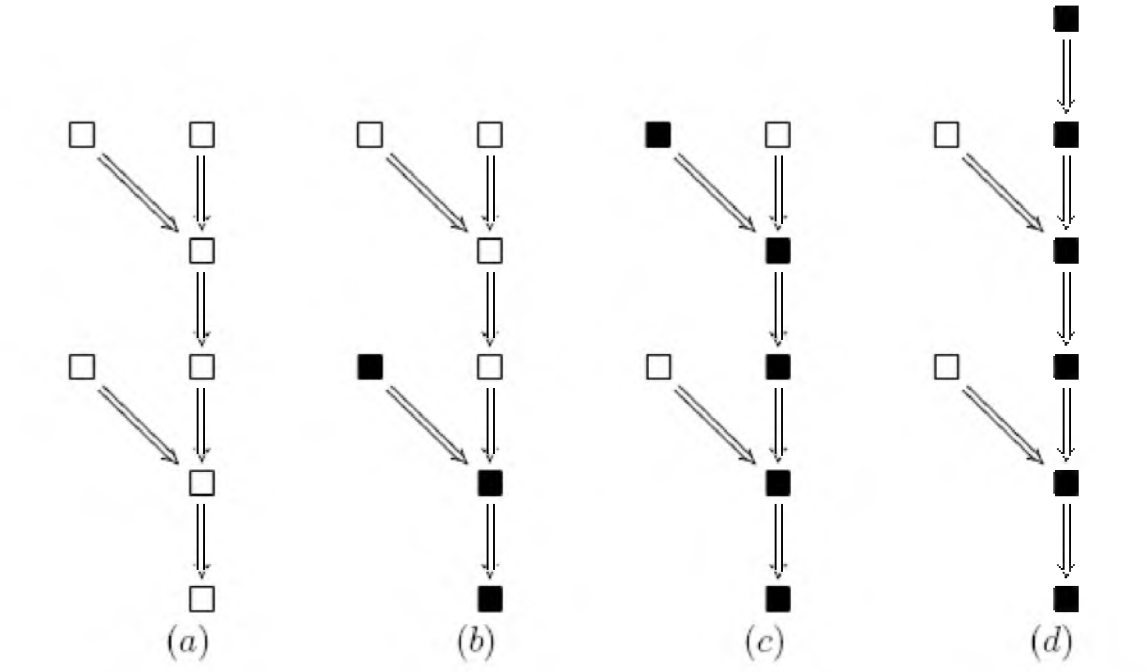

Рис. 2.2- Дерево транзакцій

Для проведення успішної атаки подвійних витрат потрібні наступні кроки:

1. Виконати транзакцію, яка використовує першу здійснену оплату.

2. Таємно майнити, використовуючи той блок, який включає в себе цю останню транзакцію.

3. Почекати, доки транзакція, що відправляє гроші продавцю отримає достатньо підтверджуючих блоків, і продавець передасть свій товар, впевнений, що гроші остаточно присвоєні йому.

4. Продовжувати майнити таємну альтернативну гілку, поки вона не стане більша, ніж публічна, після чого вона транслюється в мережу. Оскільки нова гілка довша всіх інших відомих, то вона буде вважатися

дійсною, і переведення біткойнів продавцеві буде замінений відправкою монет на іншу адресу.

Розглянемо сценарій: зловмисник намагається генерувати альтернативний ланцюг швидше, ніж основний. Навіть якщо це буде зроблено, воно не робить систему відкритою для довільних змін, таких як створення грошей з повітря або одержання грошей, які ніколи не належали атакуючому. Вузли не збираються брати недійсну транзакцію в якості оплати, і відповідно вузли мережі ніколи не приймуть блок, що їх містить. Атакуючий може тільки спробувати змінити одну з своїх угод, щоб забрати гроші, які він нещодавно витратив.

Гонку між чесним ланцюгом і атакуючим можна охарактеризувати як біноміальне випадкове блукання. Успішною подією є розширення чесного ланцюга на один блок, збільшивши свій відрив на +1, і подія невдачі - коли ланцюг атакуючого розширюється на один блок, скоротивши відставання на -1. Імовірність зловмисника наздогнати з даним відставанням аналогічна задачі про розорення гравця. Припустимо, гравець з необмеженим кредитом починає з відставанням і грає потенційно нескінченне число випробувань, щоб спробувати досягти беззбитковості. Ми можемо обчислити імовірність чи він коли-небудь досягне беззбитковості, або що зловмисник ніколи не наздожене чесного ланцюга:

Саме останній тип атаки і розглядається в даній роботі.

2.3 Аналіз Грюнспана та Накамото

Розглянемо аналіз Грюнспана щодо стійкості криптовалюти Bitcoin до атаки подвійних витрат[24].

Нехай T – випадкова величина часу, який витрачається на генерування блоку чесним майнером; T' – аналогічна випадкова величина для атакуючого.

Для визначення функції розподілу випадкових величин T та T' потрібні дві леми.

Лема 2.1.

$$P(T > t_1 + t_2) = P(T > t_1)P(T > t_2)$$

Доведення.

Випадкова величина T не залежить від пам'яті, тобто

$$P(T > t_1 + t_2 | T > t_1) = P(T > t_2)$$

Тоді, відповідно до наведеної формули ймовірності

$$P(T > t_1 + t_2) =$$

$$P(T > t_1 + t_2 | T > t_2)P(T > t_2) + P(T > t_1 + t_2 | T < t_2)P(T < t_2) =$$

$$P(T > t_1)P(T > t_2)$$

Лему доведено.

Лема 2.2 Нехай $F_T(t)$ буде функцією розподілу випадкової величини T, тобто $F_t(t) \coloneqq P(T \leq t)$.

Тоді

$$\exists\, \alpha > 0 \colon F_T(t) = 1 - e^{-\alpha t},$$

експоненціальний розподіл.

Доведення.

Визначимо $u_T(t) = P(T > t)$; тоді $F_T(t) = 1 - u_t(t)$. Звернемо увагу, що $u_t(0) = P(T > 0) = 1$.

Для певного малого $\Delta t > 0$ запишемо наступне порівняння:

$$\frac{u_T(t + \Delta t) - u_T(t)}{\Delta t} = \frac{u_T(t) \cdot u_T(\Delta t) - u_T(t)}{\Delta t} = \frac{u_T(t)(u_T(\Delta t) - u_T(0))}{\Delta t} \quad (3.1)$$

Коли $\Delta t \to 0$ в (3.1), маємо:

$$u'_T(t) = u_T(t) \cdot u'_T(0),$$

або

$$\frac{u'_T(t)}{u_T(t)} = u'_T(0),$$

$$\int \frac{du}{u_T(t)} = \int u'_T(0)dt;$$

$$\ln|u_T(t)| = u'_T(0) \cdot t + C;$$

$$u(t) = e^{u'_T(0)\cdot t + c}.$$

Але $u(0) = 0$, отже $1 = u_T(0) = e^{u'_T(0)\cdot 0} \cdot e^C => C = 0$, та $u_T(t) = e^{u'_T(0)t}$.

Також $u_T(t) = P(T > t) \leq 1 => u'_T(0) < 0$.

Тепер, приймемо

$$u'_T(0) = -\alpha, \text{де } \alpha > 0,$$

та отримуємо

$$u_T(t) = e^{-\alpha t},$$

та

$F_T(t) = 1 - e^{-\alpha t}$.

Лема доведена

Зауважимо, що для атакуючого вірний аналогічний результат:

$$\exists \alpha' > 0 \colon F_T(t) = 1 - e^{-\alpha t}.$$

Позначимо p – ймовірність, що чесного майнера обробити наступний блок раніше, за атакуючого.

Лема 2.3.

$$p = P(T < T') = \frac{\alpha}{\alpha + \alpha'}; q = P(T' < T) = \frac{\alpha'}{\alpha + \alpha'}$$

Доведення.

Зауважимо, що означення T та T' наступні:

$$f_T(t) = \alpha e^{-\alpha t};\ f_{T'}(t) = \alpha' e^{-\alpha' t}.$$

Тоді

$$q = P(T' < T) = \int\limits_{x,y:x<y} f_{T'}(x) f_T(y)\, dxdy = \int\limits_0^\infty (\int\limits_0^y f_{T'}(x)dx) f_T(y)dy$$

$$= \int\limits_0^\infty f_{T'}(y) f_T(y) dy = \int\limits_0^\infty (1 - e^{-\alpha' y}) \alpha e^{-\alpha y} dy$$

$$= \alpha \int\limits_0^\infty e^{-\alpha y} dy - \alpha \int\limits_0^\infty e^{-(\alpha+\alpha')y} dy$$

$$= -e^{-\alpha y}|_0^\infty - \left(-\frac{\alpha}{\alpha+\alpha'}\right) e^{-(\alpha+\alpha')y}|_0^\infty$$

$$= -(0-1) + \frac{\alpha}{\alpha+\alpha'}(0-1) = 1 - \frac{\alpha}{\alpha+\alpha'} = \frac{\alpha'}{\alpha+\alpha'}$$

Аналогічно (або використовуючи $p = 1 - q$), отримуємо $p = \frac{\alpha}{\alpha+\alpha'}$.

Лема доведена.

Будемо називати p частиною загальних ресурсів, який має чесний майнер, $q -$ частину ресурсів атакуючого.

$T_i -$ час, який потрібно для створення i –го блоку для чесного майнера, тобто час від події "$i - 1$й блок створено" до створення i –го.

Тоді $T_1, \dots, T_n$ – незалежні, ідентично розподілені випадкові величини з експоненціальним розподілом.

Визначимо $S_n -$ випадкова величина, час для формування n блоків, тоді $S_n = T_1 + \cdots + T_n$.

$$P(S_r < t) = F_{S_r}(t) = 1 - e^{-\alpha t} \sum_{k=0}^{n-1} \frac{(\alpha t)^k}{k!},$$

та зі щільністю розподілу

$$f_{S_r}(t) = \frac{\alpha^n}{(n-1)!} t^{n-1} e^{-\alpha t}.$$

Також визначимо $N(t) -$ випадковий процес, число блоків, створених до часу t чесним майнером.

Тоді

$$N(t) = \max\{n \geq 0 : S_r < t\}.$$

Лема 2.4. $N(t)$ має розподіл Пуассона з параметром α (або з маточікуванням αt), тобто

$$P(N(t) = n) = \frac{(\alpha t)^n}{n!} e^{-\alpha t}.$$

Доведення.

$\{N(t) = n\} = \{S_n < t \cap S_{n+1} > t\} = \{S_n < t \cap \overline{S_{n+1} < t}\} = \{S_n < t \setminus S_{n+1} < t\}.$

Але $\{S_{n+1} < t\}$ підмножина $\{S_n < t\}$, отже

$$P(N(t) = n) = P(S_n < t) - P(S_{n+1} < t) = F_{S_n}(t) - F_{S_{n-1}}(t) = \frac{(\alpha t)^n e^{-\alpha t}}{n!}.$$

Лема доведена.

Зауважимо, що для атакуючого $P(N'(t) = n) = \frac{(\alpha' t)^n e^{-\alpha' t}}{n!}$.

Лема 2.5. Нехай q_n – ймовірність події E_n наздогнати відставання в n блоків. Тоді

$$q_n = \left(\frac{q}{p}\right)^n.$$

$$P(E_n) = q_n = P\left(\frac{E_n}{T} > T'\right) P(T > T') + P\left(\frac{E_n}{T} < T'\right) P(T < T')$$

$$= P(E_{n-1})q + P(E_{n+1})p = q_{n-1}q + q_{n+1}p;$$

звідки $q_n = \left(\frac{q}{p}\right)^n$. Лема доведена.

Визначення 2.1. $X_n = N'(S_n)$ – кількість блоків, яку згенерує зловмисник за час, за який чесний майнер створить n блоків.

Лема 2.6. Випадкова величина X_n має від'ємний біноміальний розподіл з параметрами (n, p), тобто для $k \geq 0$:

$$P(X_n = k) = C_{n+k-1}^k p^n q^k$$

Доведення.

$$P(S_n \in [t, t + dt]) = F_{S_n}(t + dt) - F_{S_n}(t) = dF_{S_n}(t) := F_{S_n}^{\prime(t)} dt = f_{s_n}(t) dt$$

$$P(X_n = k) = \int_0^\infty P\left(N'(S_n) = \frac{k}{S_n} \in [t, t+dt]\right) P(S_n \in [t, t+dt])$$

$$= \int_0^\infty P(N'(t) = k) \cdot f_{s_n}(t)dt$$

$$= \int_0^\infty \frac{(\alpha' t)^k}{k!} e^{-\alpha' t} \cdot \frac{\alpha^n}{(n-1)!} t^{n-1} e^{-\alpha t} dt$$

$$= \frac{(\alpha')^k \alpha^n}{k!\,(n-1)!} \int_0^\infty t^{n-1+k} e^{-(\alpha+\alpha')t} dt = \frac{(\alpha')^k \alpha^n}{(\alpha+\alpha')^{n+k}} \cdot \frac{(k+n-1)!}{k!\,(n-1)!}$$

$$= C_{n+k-1}^k p^n q^k.$$

Лема доведена.

Аналіз Накамото. Як тільки чесний майнер створить $z-$й блок, атакуючий майнер повинен створити k блоків із ймовірністю, наведеній у наступній частині. Якщо $k > z$, то ланцюжок атакуючого довший, за основний, та атака вважається успішною. В іншому випадку йомвірність того, що їх наздожене осовна $(q/p)^2$, однак ймовірність успіху атаки P:

$$P = P[N'(S_z) \geq z] + \sum_{k=0}^{z-1} P[N'(S_z) = k] \cdot q_{z-k}.$$

Потім Накамото робить спрощуюче припущення, що блоки створюються відповідно до середнього очікуваного часу на блок. Це твердження правдиво, якщо $z \to \infty$. Він аппроксимує $N'(S_z)$ по $N'(t_z)$, де

$$t_z = E[S_z] = zE[T] = \frac{z\tau_0}{p}.$$

Випадкова величина $N'(t_z)$ має розподіл Пуассона параметром

$$\lambda = \alpha' t_z = \frac{z\alpha\tau_0}{p} = \frac{zq}{p}.$$

В результаті ймовірність за Накамото має наступний вигляд:

$$P_{SN}(z) = P[N'(t_z) \geq z] + \sum_{k=0}^{z-1} P[N'(t_z) = k] \cdot q_{z-k}$$

$$= 1 - \sum_{k=0}^{z-1} [N'(t_z) = k] + \sum_{k=0}^{z-1} P[N'(t_z) = k] \cdot q_{z-k}$$

$$= 1 - \sum_{k=0}^{z-1} e^{-\lambda} \frac{\lambda^k}{k!} (1 - q_{z-k}).$$

Але цей аналіз не є коректним при $N'(S_z) \neq N'(t_z)$.

Висновки до розділу 2

В даному розділі було наведено описання процесу функціонування криптовалюти Bitcoin, її складові та основні атаки. Також був приведений аналіз криптовалюти Грюнспана, в якому він уточнює ймовірності успіху атаки подвійних витрат, знайдені в роботі Накамото.

3. ВИЗНАЧЕННЯ МІНІМАЛЬНОЇ КІЛЬКОСТІ БЛОКІВ ПІДТВЕРДЖЕННЯ, ЩО ГАРАНТУЄ ЗБЕРЕЖЕННЯ ТРАНЗАКЦІЙ В БЛОКЧЕЙНІ З ЗАДАНОЮ ІМОВІРНІСТЮ

В даному розділі буде сформульована та доведена теорема про ймовірність успіху атаки подвійних витрат в залежності від кількості створених блоків чесним майнером, враховуючи час затримки поширення блоків у мережі. На основі неї будуть пораховані та представлені графічно кількості блоків при заданій ймовірності в залежності від хешрейту зловмисника та часу затримки поширення блоків.

3.1 Основні припущення та допоміжні твердження

Будемо використовувати ЧМ для “Чесного Майнера” та АМ для “Атакуючого Майнера”. Введемо визначення наступних випадкових величин (ВВ):

T_H – ВВ для позначення часу, за який ЧМ генерує блок,

T'_H – ВВ для позначення часу, з який блок генерується та поширюється для усіх ЧМ,

T_M – ВВ для позначення часу, за який АМ генерує блок,

T'_M – ВВ для позначення часу, за який генерується та поширюється блок, створений усіма АМ.

Як було показано у [6], випадкові величини T_M та T_H мають експоненціальні розподіли:

$$F_{T_H}(t) = P(T_H < t) = 1 - e^{\alpha_H t}, \tag{3.1}$$

$$F_{T_M}(t) = P(T_M < t) = 1 - e^{\alpha_M t},$$

для деяких $\alpha_H > 0, \alpha_M > 0$. Фізичний сенси цих параметрів такий, що $\frac{1}{\alpha_H}$ та $\frac{1}{\alpha_M}$ є середніми темпами генерації ЧМ та АМ відповідно.

Також вважатимемо, що D_H позначає час, за який ЧМ поширює блок (після генерування) до всіх вузлів у мережі (щонайменше до усіх чесних нод). Значення D_M аналогічна величина для АМ.

У даній роботі приймемо $D_M = 0$, тобто АМ зкорумпований та діє як одна особа. Це також означає, що $T'_M = T_M$ та $F_{T'_M}(t) = F_{T_M}(t)$.

Також слід зауважити, що для простоти ми приймаємо затримку часу передачі D_H однакові для усіх ЧМ. Звичайно, це певне обмеження для реальної моделі, але в альтернативному випадку неможливо враховувати всі попарні затримки. З іншого боку, ми можемо розглядати D_H як найбільшу часову затримку в мережі (для ЧМ). У цих позначеннях ми маємо

$$T'_H = D_H + T_H, T'_M = T_M. \quad (3.2)$$

Позначимо p_H ймовірність генерації блоку чесним майнером раніше за аткуючого майнера, та $p_M = 1 - p_H$ – ймовірність генерації блоку АМ швидше, ніж ЧМ.

$$p_H = \frac{\alpha_H}{\alpha_H + \alpha_M}, p_M = \frac{\alpha_M}{\alpha_H + \alpha_M}. \quad (3.3)$$

Будемо називати p_H (p_M) "частиною загального хешрейту, який має ЧМ (АМ)", відповідно до характеру цих значень. Розглянемо інші значення, які враховують час затримки $D_H > 0$:

p'_H – ймовірність, з якою ЧМ згенерує та поширить наступний блок усім (принаймні чесним) нодам раніше, ніж АМ згенерує наступний блок,

p'_M – ймовірність альтернативного сценарія, $p'_M = 1 - p'_H$.

Тоді

$$p'_H = P(T'_H < T_H), p'_M = P(T'_M < T_M) \tag{3.4}$$

та $p'_H + p'_M = 1$.

Ці два значення (3.4) мають значно більшу важливість, ніж (3.3), оскільки вони враховують час затримки D_H та набагато більш реально описують стан мережі. Далі ми покажемо, що ймовірність успішної атаки залежить від значень (3.4), а не від значень (3.3). Таким чином, якщо D_H досить велика, то "справжній" хешрейт p'_H ЧМ істотно менше, ніж p_H.

Тепер знайдемо p'_H та p'_M.

Лемма 3.1. В наших позначеннях

$$p'_H = e^{-\alpha_M D_H} \cdot \frac{\alpha_H}{\alpha_H + \alpha_M} = e^{-\alpha_M D_H} \cdot p_H,$$
$$p'_M = 1 - e^{-\alpha_M D_H} \cdot \frac{\alpha_H}{\alpha_H + \alpha_M} = 1 - e^{-\alpha_M D_H} \cdot p_H \tag{3.5}$$

Доведення. Зауважимо, що функції розподілу випадкових величин T'_H та T_H відповідно до (2) та (4) є:

$$F_{T'_H}(t) = P(T'_H < t) = P(T_H + D_H < t) = P(T_H < t - D_H)$$
$$= \begin{cases} 1 - e^{-\alpha_H(t-D_H)}, \text{якщо } t > D_H, \\ 0, \quad \text{в іншому випадку;} \end{cases} \tag{3.6}$$

$$F_{T_M}(t) = 1 - e^{\alpha_M t}. \tag{3.7}$$

Відповідними щільностями є

$$f_{T'_H}(t) = \alpha_H e^{-\alpha_H(t-D_H)},$$
$$f_{T_M}(t) = \alpha_H e^{-\alpha_M t}. \tag{3.8}$$

Тоді, за формулою повної ймовірності,

$$p'_M = P(T_M < T_H) = P\left(T_M < \frac{T_H}{T_M} < D\right) P(T_M < D) + \\ + P(T_M < T_H / T_M D) P(T_M < D). \tag{3.9}$$

Але $P\left(T_M < \frac{T'_H}{T_M} < D_H\right) = 1$ тому, що з (3.2) ми отримуємо $T_H \geq D_H$. Отже

$$p'_M = P(T_M < D_H) + P(D_H < T_M < T'_H).$$

Далі, відповідно до (3.5) – (3.8) маємо

$$P(T_M < D_H) = 1 - e^{-\alpha_M D_H};$$

$$P(D_H < T_M < T'_H) = \int\limits_{x,y: D_H < x < y} f_M(x) f_{T_H}(y) dx dy$$

$$= \int_{D_H}^{\infty} \left(\int_{D_H}^{y} f_M(x) dx \right) f_{T'_H}(y) dy$$

$$= \int_{D_H}^{\infty} (F_M(y) - F_M(D_H)) f_{T_H}(y - D_H) dy$$

$$= \int_{D_H}^{\infty} (1 - e^{-\alpha_M y} - (1 - e^{-\alpha_M D_H})) \alpha_H e^{-\alpha_H (y - D_H)} dy$$

$$= \int_{D_H}^{\infty} (e^{-\alpha_M D_H} - e^{-\alpha_M y}) \alpha_H e^{-\alpha_H (y - D_H)} dy$$

$$= \alpha_H e^{-\alpha_M D_H} \int_{D_H}^{\infty} (1 - e^{-\alpha_M (y - D_H)}) e^{-\alpha_H (y - D_H)} dy$$

$$= \alpha_H e^{-\alpha_M D_H} \int_{0}^{\infty} (1 - e^{-\alpha_M z}) e^{-\alpha_H z} dz,$$

де $z = y - D_H$.

Після інтегрування отримуємо

$$P(D_H < T_M < T'_M) = \alpha_H e^{-\alpha_M D_H} \cdot \frac{\alpha_M}{\alpha_H + \alpha_M},$$

та з (3.9) маємо

$$P'_M = 1 - e^{-\alpha_M D_H} + e^{-\alpha_M D_H} \cdot \frac{\alpha_M}{\alpha_H + \alpha_M} = 1 - e^{-\alpha_M D_H} \cdot \left(1 - \frac{\alpha_M}{\alpha_H + \alpha_M}\right)$$

$$= 1 - e^{-\alpha_M D_H} \cdot \frac{\alpha_H}{\alpha_H + \alpha_M} = 1 - e^{-\alpha_M D_H} \cdot p_H.$$

Відповідно, $p'_H = 1 - p'_M = e^{-\alpha_M D_H} \cdot p_H$, та формула (3.4) та лема доведені.

Лема 3.1 має велике значення, так як вона показує, що нерівність

$$p'_M > p'_H \tag{3.10}$$

є еквівалентом ситуації, коли АМ мають справжню більшість і можуть виконати "атаку 50%" навіть якщо $p_H > p_M$, оскільки за умови (3.10) атакуючий ланцюжок буде зростати швидше.

Іншими словами, коли D_H досить великий, атака 50% може відбутися навіть у випадку, якщо ЧМ володіє переважною обчислювальною потужністю. Точніше, як буде показано нижче, необхідна та достатня умова для успіху атаки 50, це умова (3.10) замість $p_M > p_H$. Ми також можемо переписати (3.10) у формі

$$1 - e^{-\alpha_M D_H} \cdot p_H < e^{-\alpha_M D_H} \cdot p_H,$$

що еквівалентно нерівності

(3.11)

$$D_H > \frac{ln(2p_H)}{\alpha_M},$$

що також необхідна та достатня умова для атаки 50%. Формула 11 визначає межу часу затримки D_H для цієї атаки.

3.2 Ймовірність успіху атаки подвійних витрат в залежності від затримки прийняття блоків у мережі

У цій частині ми формулюємо основні результати після деяких допоміжних лем.

Позначимо $T'_H(i)$ як час, необхідний для генерації та поширення у мережі чесним майнером $i-$го блоку, тобто час від події "$i-1$-й блок створений та доступний для всіх вузлів" до "i-й блок створений та доступний для всіх вузлів". Як і у (3.2), ми можемо сказати, що

$$T'_H(i) = T_H(i) + D_H, \tag{3.12}$$

де $T_H(i)$ – час, потрібний ЧМ для генерації i-го блоку (після того, як $i-1$-й блок став доступний). Тоді $T'_H(i), i \geq 1$ – незалежна однаково розподілена випадкова величина з функцією розподілу

$F_{T'_{H(i)}}(t) = F_{T'_H}(t) = F_{T'_H}(t - D_H) = 1 - e^{-\alpha_H(t-D_H)}$, для усіх $i \geq 1$,

де остання рівність слідує з (3.1).

Також, аналогічно позначимо випадкову величину $T_M(i), i \geq 1$. Їх функції розподілу

$$F_{T_{M(i)}}(t) = 1 - e^{-\alpha_M t}, \text{для усіх } i \geq 1.$$

Також, для $n \geq 1$ визначим випадкову величину $S_H(n)$, де

$$S_H(n) = \sum_{i=1}^{n} T_H(i), \tag{3.13}$$

та випадкові величини $S'_H(n)$

$$S'_H(n) = \sum_{i=1}^{n} T'_H(i). \tag{3.14}$$

Тоді $S_H(n)$ – час, потрібний для генерації (без поширення) n (незалежних) блоків, та $S'_H(n)$ – час для генерації та поширення чесним майнером n блоків підряд.

З (3.12) отримуємо наступне:

$$S'_H = S_H(n) + nD_H,$$

де $S_H(n)$ має розподіл Ерланга як сума незалежних однаково розподілених випадкових величин з експоненціальним розподілом:

$$F_{S_H(n)}(t) = P(S_H(n) \leq t) = 1 - e^{-\alpha_H t} \sum_{i=1}^{n} \frac{(\alpha_H t)^k}{k!}. \quad (3.15)$$

Також, визначим випадкову величину $S_M(n)$ аналогічним чином**:**

$$S_M(n) = \sum_{i=1}^{n} T_M(i). \quad (3.16)$$

Зауважимо, що $S_M(n)$ також має розподіл Ерланга:

$$F_{S_M(n)}(t) = 1 - e^{-\alpha_M t} \sum_{i=1}^{n} \frac{(\alpha_M t)^k}{k!}. \quad (3.17)$$

Також визначимо випадкову величину $N_M(t)$ як кількість блоків, створених атакуючим майнером до моменту часу t.

*Леммма 3.2***:** випадкова величина $N_M(t)$ має розподіл Пуасон з параметром α_M:

$$P(N_M(t) = n) = \frac{(\alpha_M t)^n e^{-\alpha_M t}}{n!}. \quad (3.18)$$

Доведення. Подія $\{N_M(t) = n\}$ така ж, як і подія $\{S_M(n) < t\} \cap \{S_M(n+1) > t\}$, де $S_M(n)$ була визначена в (3.16). Отже, ми можемо написати наступний ланцюжок порінянь:

$$\{N_M(t) = n\} = \{S_M(n) < t \cap S_M(n+1) > t\} = \{S_M(n) < t \cap \overline{S_M(n+1) < t}\}$$
$$= \{S_M(n) < t\} \backslash \{S_M(n+1) < t\}.$$

Але, відповідно до визначення (16), $\{S_M(n+1) < t\} \subset \{S_M(n) < t\}$, використовуючи (3.17)

$$P\{N_M(t) = n\} = P\{S_M(n) < t\} - P\{S_M(n+1) < t\} = F_{S_M(n)}(t) - F_{S_M(n+1)}(t)$$
$$= \frac{(\alpha_M t)^n e^{-\alpha_M t}}{n!}.$$

Лема доведена.

Примітка 3.1: із властивостей процессу Пуассона (незалежні прирости, відсутність післяефектів), отримуємо, що для всіх $t_1, t_2 > 0$:

(3.19)

$$N_M(t_1 + t_2) = N_M(t_1) + N_M(t_2).$$

Визначимо випадкову величину

$$X'_M(n) = N_M\big(S'_H(n)\big), \tag{3.20}$$

яка позначає кількість блоків, яку згенерує АМ за час, за який ЧМ згенерує та поширить n блоків.

Також, введемо випадкову величину

$$X_M(n) = N_M\big(S_H(n)\big) \tag{3.21}$$

аналогічним чином.

Знайдемо функцію розподілу випадкової величини $X'_M(n)$.

Лемма 3.3: визначимо

$$P_n(k) = P(X'_M(n) = k). \tag{3.22}$$

Наступні твердження правдиві:

1. ВВ $X'_M(n)$ є сумою двох випадкових величин:

$$X'_M(n) = X_M(n) + N_M(nD_n) = N_M\big(S_H(n)\big) + N_M(nD_n), \tag{3.23}$$

де $S_H(n)$ та $X_M(n)$ були визначені в (3.13) та (3.21) відповідно.

2. ВВ $N_M\big(S_H(n)\big)$ має від'ємний біноміальний розподіл з параметрами (n, p_H), та ВВ $N_M(nD_n)$ має розподіл Пуассона з параметром $\alpha_M nD_n$:

$$P\left(N_M\big(S_H(n)\big)\right) = C_{n+k-1}^{k} p_H^n p_M^k, \tag{3.24}$$

$$P(N_M(nD) = k) = \frac{e^{-\alpha_M nD_H} \cdot (\alpha_M nD_H)^k}{k!}. \tag{3.25}$$

3. Розподіл ймовірності для ВВ $X'_M(n)$:

$$P_n(k) = \frac{p_H^n}{(n-1)!} \cdot \frac{e^{-\alpha_M nD_H} \cdot (\alpha_M nD_H)^k}{k!} \cdot \sum_{i=0}^{k} \frac{(n-i+1)! \cdot C_k^i}{(\alpha nD_H)^i}, \tag{3.26}$$

де

$$\alpha = \alpha_M + \alpha_H. \tag{3.27}$$

Доведення.

1. Відповідно до означень (3.20), (3.12) та (3.14) отримуємо:

$$X'_M(n) = N_M\big(S'_H(n)\big) = N_M(S_H(n) + nD_n) = N_M\big(S_H(n)\big) + N_M(nD_n),$$

де остання рівність була приведена раніше, отже (23) доведено.

2. Для доведення (3.24) зауважимо, що ВВ $N_M\big(S_H(n)\big)$ аналогічна до ВВ X_n зі статті Грюнспана, яка має від'ємний біноміальний розподіл з параметрами (n, p_H). Далі, відповідно до лемми 3.2, $N_M(nD_n)$ має розподіл Пуассона з параметром α_M, звідки ми отримуємо (3.25).

3. Відповідно до 2-ї частини даної лемми,

$$N_M\big(S'_H(n)\big) = N_M\big(S_H(n)\big) + N_M(nD_n),$$

де дві ВВ в правій частині рівності незалежні. Отже, сума цих значень має розподіл, який є згорткою їх розподілів

$$P_n(k) = \sum_{i=0}^{k} P(N_M(S_H(n)) = i) \times P(N_M(nD_n)) = k - i)$$

$$= \sum_{i=0}^{k} \left\{ C_{n+i-1}^{i} p_H^n p_M^i \frac{e^{-\alpha_M n D_H} \cdot (\alpha_M n D_H)^{k-i}}{(k-i)!} \right\}$$

$$= \frac{p_H^n}{(n-1)!} \cdot \frac{e^{-\alpha_M n D_H} \cdot (\alpha_M n D_H)^k}{k!} \cdot \sum_{i=0}^{k} \frac{(n-i+1)! \cdot C_k^i}{(\alpha n D_H)^i},$$

де $\alpha = \alpha_M + \alpha_H$. Лемма повністю доведена.

Лемма 4: нехай q_n – ймовірність події E_n, наздогнати n блоків.

Тоді

$$q_n = \begin{cases} 1, \text{якщо } p'_M \geq p'_H, \\ \left(\frac{p'_M}{p'_H}\right)^n = \left(\frac{\alpha_M + \alpha_M(1 - e^{-\alpha_M D_H})}{\alpha_H e^{-\alpha_H D_H}}\right)^n \end{cases} \quad (3.28)$$

Доведення. Використовуючи формулу повної ймовірності, отримаємо:

$$q_n = P(E_n) = P(E_n / T'_H > T'_M) P(T'_H > T'_M)$$
$$+ P(E_n / T'_H < T'_M) P(T'_H < T'_M) = P(E_{n-1}) p'_M + P(E_{n+1}) p'_H,$$

де остання рівність отримана, використовуючи лемму 1.

Можна переписати даний вираз як:

$$q_n = q_{n-1} p'_M + q_{n+1} p'_H. \quad (3.29)$$

Для вирішення (3.29) застосуємо характеристичне рівняння

$$\lambda^2 p'_H - \lambda + p'_M = 0,$$

коренями якого є $\lambda_1 = 1$ та $\lambda_2 = \frac{p'_M}{p'_H}$. Отже, загальний розв'язок (3.29):

$$q_n = a\lambda_1^n + b\lambda_2^n = a + b\left(\frac{p'_M}{p'_H}\right)^n.$$

Якщо $p'_M > p'_H$, тоді $\frac{p'_M}{p'_H} > 1$. Але $0 \leq q_n \leq 1$, отже в цьому випадку єдиний розв'язок це $q_n = 1$.

Далі, у випадку $p'_M = p'_H = \frac{1}{2}$ отримаємо рівняння

$$\lambda^2 - 2\lambda + 1 = 0,$$

звідки $\lambda_1 = \lambda_2 = 1$ та $q_n = 1$ для $n \geq 1$, використовуючи початковий стан $q_0 = 1$.

В результаті, якщо $p'_M < p'_H$, з граничних умов $q_0 = 1, q_\infty = 0$ отримуємо $a = 0, b = 1$ та

$$q_n = \left(\frac{p'_M}{p'_H}\right)^n. \tag{3.28}$$

Лема доведена.

Тепер сформулюємо головний результат даної роботи.

Теорема 1: Ймовірність успіху атакуючого майнера після z підтверджених блоків, згенерованих чесним майнером становить:

$$(z) = \begin{cases} 1, \text{якщо } p'_M \geq p'_H, \\ 1 - \sum_{k=0}^{z} P_z(k)\left(1 - \left(\frac{p'_M}{p'_H}\right)^{z-k}\right), \text{інакше.} \end{cases}$$

Доведення. Для певного сталого z визначимо подію $A_z(k)$ як

$$A_z(k) = \left\{\bigcup_{k>z} A_z(k)\right\} \cup \left\{\bigcup_{k=0}^{z-1}(A_z(k) \cap E_{n-k})\right\},$$

де подія E_{z-k} була введена у леммі 3.4.

Зауважимо, що події $\{\bigcup_{k>z} A_z(k)\}$ та $\{\bigcup_{k=0}^{z-1}(A_z(k) \cap E_{n-k})\}$ не перетинаються, і події $A_z(k)$ та E_{n-k} незалежні. Відповідно до лемми 3.3, $P(A_z(k)) = P_n(k)$, та відповідно до лемми 4, $P(E_{z-k}) = \left(\frac{p'_M}{p'_H}\right)^{z-k}$.

Використовуючи дві дані рівності, отримуємо:

$$P(A_z) = \sum_{k=z}^{\infty} P\big(A_z(k)\big) + \sum_{k=0}^{z-1} P\big(A_z(k)\big) \cdot P(E_{z-k})$$

$$= 1 - \sum_{k=0}^{z-1} P\big(A_z(k)\big) + \sum_{k=0}^{z-1} P\big(A_z(k)\big) \cdot P(E_{z-k})$$

$$= 1 - \sum_{k=0}^{z-1} P\Big(A_z(k)\big(1 - P(E_{z-k})\big)\Big) = 1$$

$$- \sum_{k=0}^{z} P_z(k) \left(1 - \left(\frac{p'_M}{p'_H}\right)^{z-k}\right),$$

теорема доведена.

3.3 Числові результати

Наведемо числові результати попереднього підрозділу.

Таблиця 3.1. Результати для $\alpha_H = 0.00167$ та різних значень хешрейту зловмисника та часу синхронізації.

p_m	$D_H = 0$	D_H=15	D_H=30	D_H=60	D_H=120	D_H=180
	Z					
0.1	6	6	6	6	7	7
0.15	9	9	9	9	10	11
0.2	13	13	14	14	16	17
0.25	20	20	21	22	26	30
0.3	32	33	35	39	48	61
0.35	58	62	67	78	111	176
0.4	133	150	170	224	515	$P_{успіху} = 1$

На рисунку 3.1 зображена залежність кількості підтверджень, яка необхідна для ймовірності успіху атаки $1/1000$ в залежності від хешрейту атакуючого. Час генерації блоку становить 600 секунд – середній час генерування блоку криптовалюти Bitcoin.

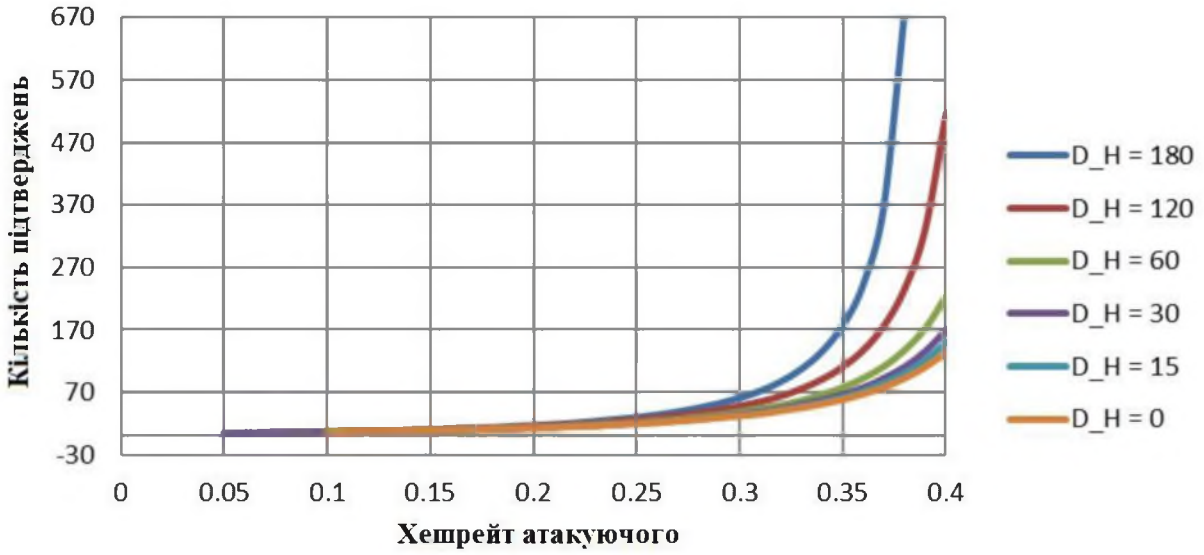

Рисунок. 3.1 – Кількість підтверджень для ймовірності успіху атаки 1/1000.

Таблиця 3.2. Результати для $\alpha_H = 0.0167$ та різних значень хешрейту зловмисника та часу синхронізації.

p_m	$D_H = 0$	$D_H = 5$	$D_H = 15$	$D_H = 30$	$D_H = 60$
	Z				
0.1	6	6	7	8	10
0.15	9	9	11	13	19
0.2	13	14	17	22	42
0.25	20	22	28	43	172
0.3	32	37	54	113	$P_{успіху} = 1$
0.35	58	74	137	$P_{успіху} = 1$	

Представимо результати обчислень графічно. На рисунках 3.2 та 3.3 зображена залежність ймовірності успіху атаки на криптовалютю Біткойн від хешрейту атакуючого, враховуючи затримку поширення блоку в мережі для різного часу генерації блоків системою.

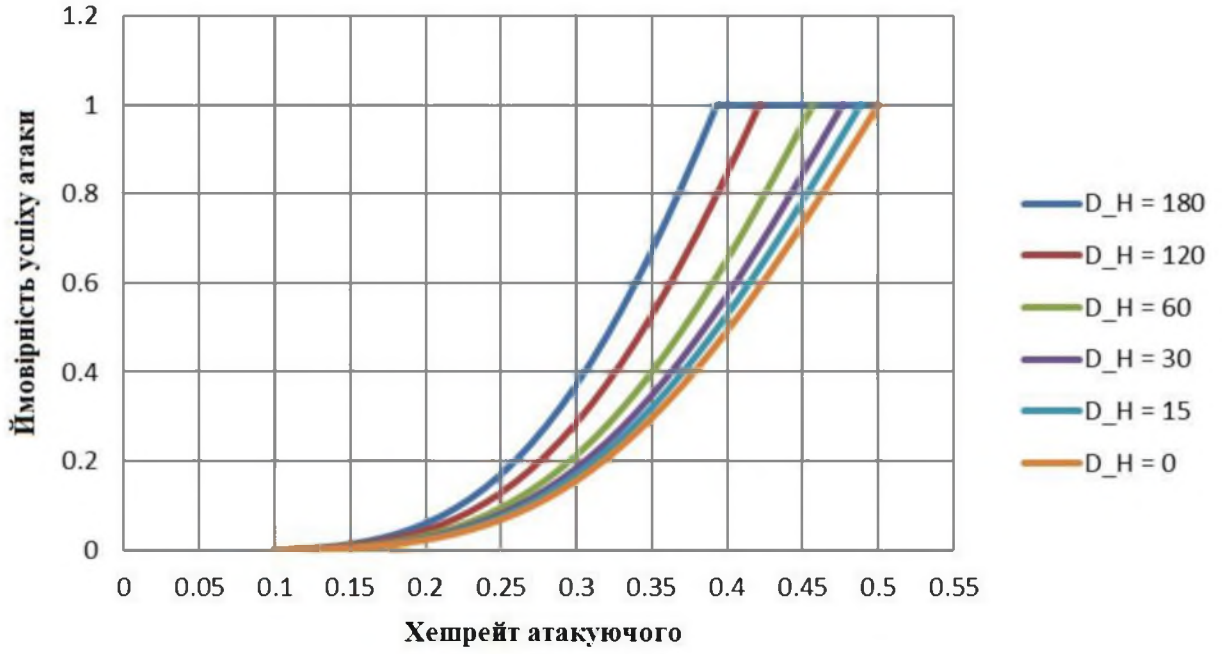

Рисунок 3.2 – Ймовірність успіху атаки (генерація блоку 600 секунд, 6 підтверджень)

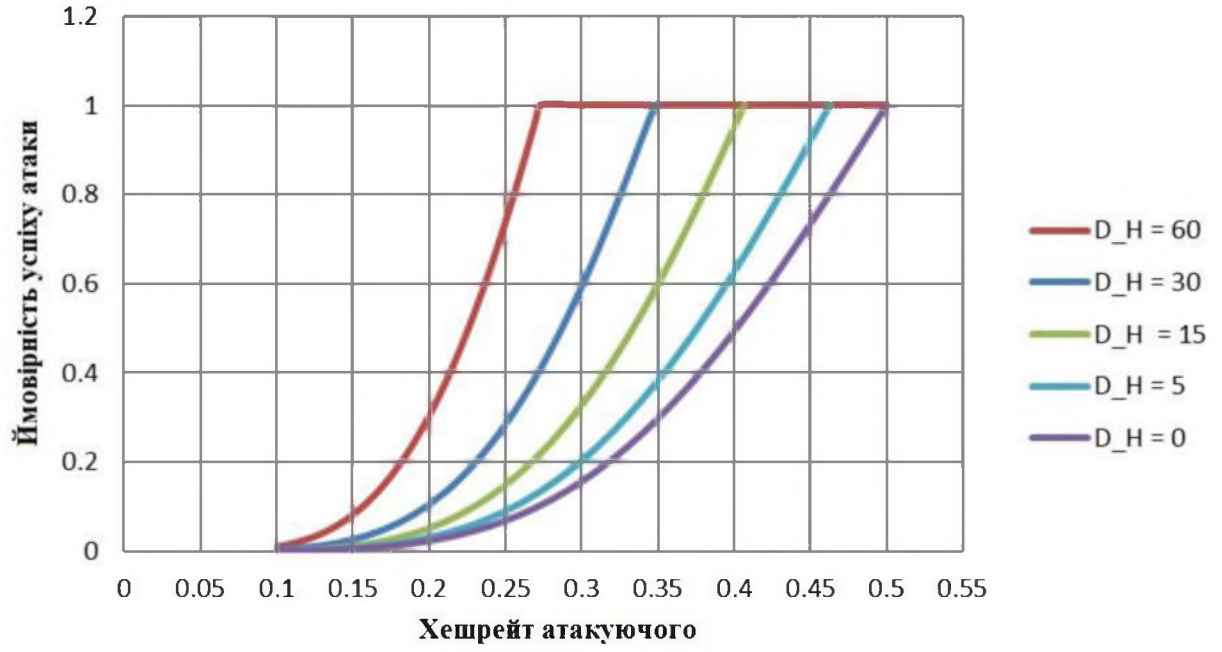

Рисунок 3.3 – Ймовірність успіху атаки (генерація блоку 60 секунд, 6 підтверджень)

На рисунку 3.1 зображено експоненціальне зростання необхідної кількості підтверджень блоків для успішної атаки при збільшенні часу поширення блоку у мережі (принаймні до всіх чесних майнерів).

Висновки до розділу 3

В даному розділі було сформульовано теорему для ймовірності успіху атаки подвійних витрат на криптовалюту Bitcoin із залежністю до часу затримки поширення блоку у мережі. Для досягнення мети було сформульовано та доведено декілька допоміжних лемм та введена певна кількість означень. Для формули ймовірності успіху атаки були отримані чисельні результати.

ВИСНОВКИ

У даній дипломній роботі було розглянуто систему ланцюжків блоків транзакцій. Після створення даної структури в протоколі криптовалюти Bitcoin, з'явилася велика кількість децентралізованих систем на базі ланцюжків блоків транзакцій. Значне поширення серед різних сфер застосування робить дослідження нових можливостей та вразливостей надзвичайно актуальною задачею.

Також була детально розглянута криптовалюта Bitcoin. Аналіз цієї криптовалюти дає змогу узагальнити факти також для багатьох інших криптовалют, адже велика кількість була створена на базі системи функціонування Bitcoin. Був приведений розгляд атак на систему Bitcoin, які можуть бути реалізовані також на подібні криптовалюти, при виконанні певних умов.

В даній роботі була знайдена залежність ймовірності успіху атаки подвійних витрат після створення певної кількості блоків від часу поширення у мережі. На основі даної теореми були отримані значення кількостей блоків підтвердження в залежності від часу поширення у мережі при заданих значенях ймовірності успіху атаки. Чисельні результати зображені в таблицях та на рисунках і підтверджують відповідність нашої моделі до реальності. На графіках видно експоненціальне зростання потрібної кількості підтверджень блоків при збільшенні затримки поширення блоків у мережі для заданої ймовірності успіху атаки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Sunny King and Scott Nadal. “Ppcoin: Peer-to-peer crypto-currency with proof-of-stake”,19,04,2012

2. King, S.; Nadal, S. (August 12, 2012)."PPCoin: Peer-to-peer crypto-currency with proof-of-stake"

3. "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies", Homeland Security Governmental Affairs, 18.10.2013

4. Liu, Debin; Camp, L. Jean (June 2006). "Proof of Work can work". Fifth Workshop on the Economics of Information Security.

5. Marino, B., Juels, A.: Setting standards for altering and undoing smart contracts. In: RuleML. pp. 151{166 (2016)

6. "Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury Before the United States Senate Committee on Banking, Housing, and Urban Affairs Subcommittee on National Security and International Trade and Finance Subcommittee on Economic Policy". *fincen.gov*. Financial Crimes Enforcement Network. 19 November 2013.

7. Andy Greenberg (20 April 2011). "Crypto Currency". Forbes.com.

8. Дэвид Чом: «Цифровая наличность заменит бумажную!» — Журнал «Компьютерра», #33 від 17.08.1999

9. Bitcoin developer chats about regulation, open source, and the elusive Satoshi Nakamoto, PCWorld, 26-05-2013

10. What is Bitcoin Mining?, The Genesis Block, 26-05-2013

11. Isgur, Ben (2014-07-16). "A Little Altcoin Sanity: Namecoin"

12. Charlton, Alistair (2013-11-28). "Litecoin value leaps 100% in a day as market cap passes $1bn". *International Business Times, UK Edition*.

13. King, S.; Nadal, S. (August 12, 2012)."PPCoin: Peer-to-peer crypto-currency with proof-of-stake"

14. "Croatia considers Bitcoin legal; 45 members of the Swiss parliament want the same", M.Santos, 10.12.2013, The 99 BITCOINS

15. "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies", Homeland Security Governmental Affairs, 18.10.2013

16. Zerocoin: Anonymous Distributed E-Cash from Bitcoin, The Johns Hopkins University Department of Computer Science, 26-05-2013

17. Марк Андрессен. Why Bitcoin Matters // The New York Times 21.01.2014

18. "Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity", 24.04.2012, Directorate of Intelligence, FBI.

19. Jon Matonis. Be Your Own Bank: Bitcoin Wallet for Apple, Forbes (26 April 2012)

20. Joshua Kopstein (12 December 2013). "The Mission to Decentralize the Internet". The New Yorker.

21. Andreas M. Antonopoulos (April 2014). Mastering Bitcoin. Unlocking Digital Crypto-Currencies. O'Reilly Media.

22. "What the 'Bitcoin Bug' Means: A Guide To Transaction Malleability", Danny Bradbury, CoinDesk, 12.02.2014

23. Douceur, John R. (2002). "The Sybil Attack"

24.CYRIL GRUNSPAN AND RICARDO PEREZ-MARCO (09.02.2017). “DOUBLE SPEND RACES”.